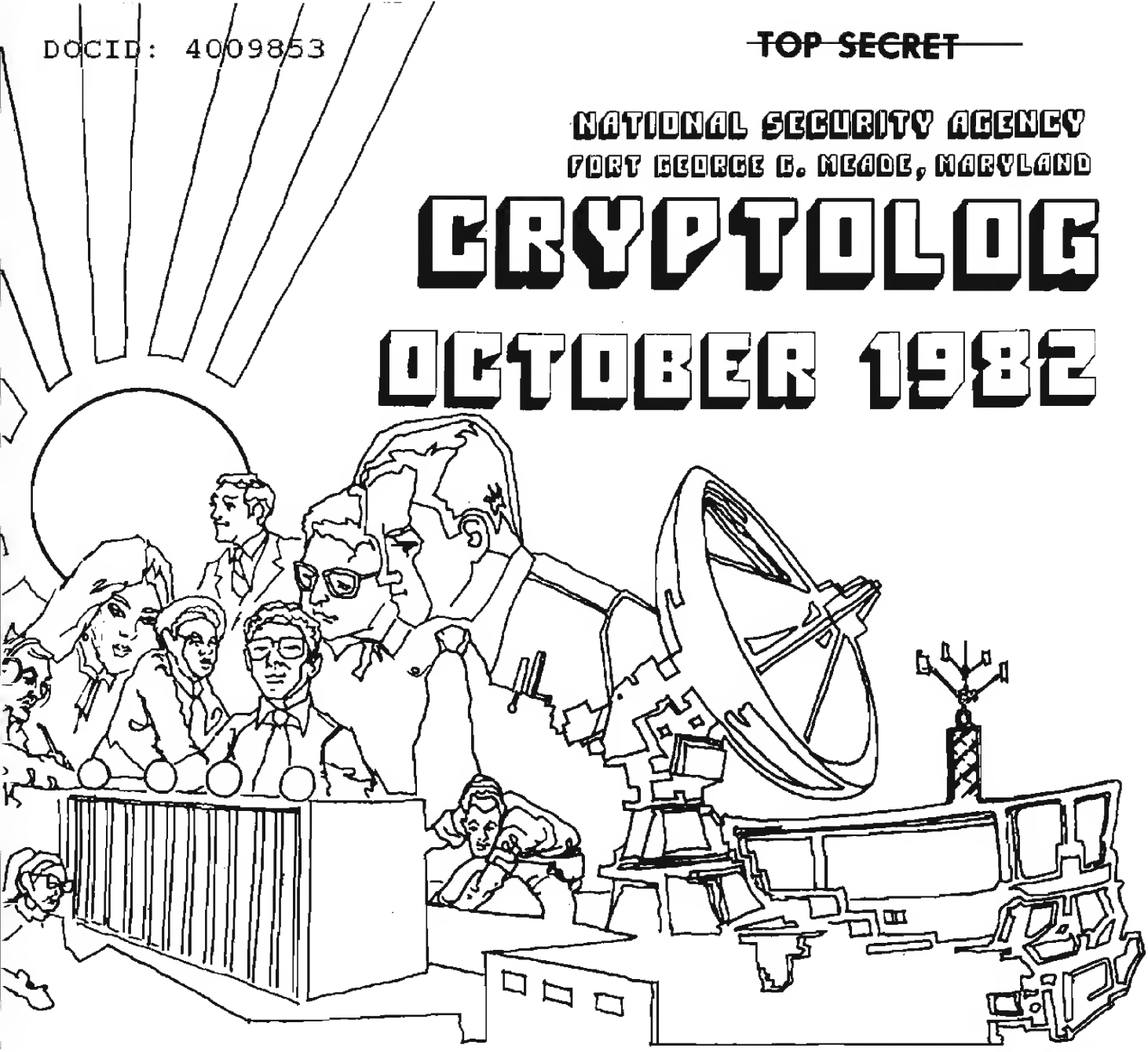
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1982



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 10 OCTOBER 1982

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlc@5
(bar-one-c-zero-five)
(note: no '0' in 'log')

NOTE:

The front cover of the September 1982 issue should carry the caveat:

Not Releasable To Contractors

Editorial

"Can two walk together unless they are agreed?" And can they agree unless they communicate? Many of the tasks we find ourselves confronted with these days require a multi-skilled approach. From the manager's point of view, it would be nice to have a lot of multi-skilled people around, so that when a problem came up, one could decide just what mix of skills were needed and then order the proper multi-skilled person(s) to go in and solve the problem. We might even set up a data base and query the computer....

Although managers continue to ask for multi-skilled people to do these tasks, it seems clear that most people learn only one skill at a time. Therefore, most of these tasks requiring a multi-skilled approach must be attacked by using two or more people, each with different skills.

Supervising a group of people with similar skills and perspectives is hard enough, but trying to manage a group of people with various skills and viewpoints is often much harder, especially if the supervisor doesn't have all of those skills. That is probably why managers keep asking for multi-skilled people.

Part of the problem lies in communications. When we talk with people in other skill fields, we may think we use the same language. Mostly, we use the same words--with different meanings. Each skill area develops its own working dialect, borrowing words and changing their meaning to fit the skill area. The answer probably lies in listening to one another.

LEADERSHIP: A Personal Philosophy (U)

by [redacted] G12

P.L. 86-36

Each member of the Class of 1982, Army War College, was required to prepare a paper setting forth a personal philosophy of leadership which best met the challenge of a senior leadership position in his organization or agency. This paper was selected by the faculty for publication and is reprinted here by permission of the author.

Leadership has received much attention in recent years from various writers and research groups. The question of how we get people to cooperate on a common task for the purpose of achieving a shared goal has always been a major problem for mankind. Concern with this question has mounted as the complexity of tasks in our world has increased to the point where relatively few jobs can be accomplished by an individual working alone.

Leadership has been defined in several ways by those who have worked in this area:

> "Leadership is the exercise of authority and the making of decisions." (Dubin, 1951)
>
> "The leader is the person who creates the most effective change in group performance." (Cattell, 1951)
>
> "The leader is one who succeeds in getting others to follow him." (Cowley, 1928)
>
> "Leadership is the process of influencing group activities toward goal setting and goal achievement." (Stogdill, 1948)

Two important threads run through all of the above definitions. The first is that leadership is a relationship between people in which influence and power are unevenly distributed. The second observation is that there can be no leaders in isolation. If you want to know whether you are a leader, see if there is someone following you. The difference that makes the difference between successful and unsuccessful leaders is of great importance to me, and I'm sure to the other students here at the War College, as we move towards higher-level civilian and military positions.

THEORETICAL CONSIDERATIONS OF LEADERSHIP

Leadership is always a relative process. To be effective and to communicate as intended, a leader must always adapt his behavior to take into account the expectations, values, and interpersonal skills of those with whom he is interacting. There can be no specific rules of leadership which will work well in all situations. Broad principles can be applied in the process of leadership and furnish valuable guides to behavior. These principles, however, must be applied always in a manner that takes fully into account the characteristics of the specific situation and of the people involved.

It is possible to state principles of leadership in such a way that they are incapable of empirical refutation and appear equally consistent with quite different forms of leader behavior. To say that a leader should manage in such a way that personnel at all levels feel real responsibility for the attainment of the organization's goals (Likert, 1967) or alternatively, that he should exhibit concern for both production and people (Blake and Mouton, 1964), is not saying a great deal about what he should do in the concrete situations that he faces daily.

The increasing tempo of our social evolution requires improved human relations techniques and increased knowledge of the social sciences in contrast to the greater emphasis on mechanical techniques and the natural sciences in the past. To cope effectively with these shifting demands, the successful leader must have a keen sense of timing and adaptation. He must learn to "roll with the punch" and yet maintain a gyroscopic guidance for the organization, keeping it within the confines of fundamental principles and headed toward a sound objective.

Over the past three decades, research has been conducted into the relationships between the four styles of leadership

- high-initiating-structure, low-consideration;
- high-initiating-structure, high-consideration;
- low-initiating-structure, high-consideration;
- low-initiating-structure, low-consideration,

productivity, and employee satisfaction. The findings were neither consistent nor definitive. The major conclusion that can be drawn from these studies is that, as previously stated, there is no one best style that is appropriate for all situations.

HOW WE CAN GET THERE FROM HERE OR HOW I WOULD RUN (MANAGE) MY AGENCY

My initial thoughts on how I would run such a massive intelligence organization as the National Security Agency coincided, to a large degree, with those functions of an executive as delineated in numerous writings on administration. These leadership duties essentially are as follows:

1. Planning: determining what should be done--including clarification of objectives, establishment of policies, mapping of programs, and determining methods and procedures.

2. Organizing: grouping the activities necessary to carry out the plans into administrative units, and defining the relationships among the executives and workers in such units.

3. Assembling resources: obtaining the personnel, capital, facilities, and other things needed to execute the plans.

4. Directing (issuing instructions): Indicating plans to those who are responsible for carrying them out, and stressing personal relationships between the "boss" and his subordinates.

5. Controlling: seeing that operating results conform as nearly as possible to the plans--the establishment of standards, motivation of people to achieve these standards, comparison of actual results against the standard, and necessary corrective action where performance deviates from the plan.

However, after some intensive reflection on this subject, other salient aspects began to emerge which embrace, if you will, my personal philosophy of leadership. Firstly, I believe that leadership is the process of influencing a group or getting others to accomplish things. A leader doesn't necessarily have to solve problems; rather, his job is to get problems solved. TO MAKE POLICY IS EASY; TO MAKE IT HAPPEN IS DIFFICULT. During my twenty years as an analyst at NSA, I have been exposed to a variety of managers, some good and some not so good. The manager I have the greatest respect for is an individual who:

(a) delegated responsibility to me without hesitation;

(b) trusted me fully;

(c) listened intently to problems and recommended solutions; and

(d) supported me completely.

If I occupied the top position at NSA, I would make every effort to emulate my favorite manager's leadership style to the maximum extent possible. One of the most important things that I learned from him was that the higher your position is, the more (no less) dependent you become on others.

Secondly, I believe that a leader must be courageous and possess the ability to make rapid but sound decisions. As you are aware, intelligence information come from a variety of sources and is often fragmented and incomplete. Even in the absence of complete and vital data, I would not hesitate in making the critical decision required. Remember, the moment of absolute certainty never arrives. One can never be 100 percent sure of anything.

Thirdly, I can not overemphasize my feeling that leadership style must rise above day-to-day activities. I strongly believe that a leader must have the mental agility and the creative vision to conceptualize how "things come together." As the Director, NSA, I would make a concerted effort to instill in my subordinates that in order to become effective leaders, they must possess the courage to dream, the ability to organize, and the strength to execute. My first step would be to host an informal gathering of my top-level executives (Office Chiefs for Planning, Operations, Budgeting, Research and Development, COMSEC, etc.) at some secluded location that was conducive to relaxation and reflective thinking. To set the tone for this session, I would cite some inspirational remarks made by the following outstanding leaders who were truly men of vision:

"Ask not what your country can do for you, but what you can do for your country."

John F. Kennedy

"I have a dream...."

Martin Luther King

"Some men see things as they are and say why. I dream things that never were and say why not."

Robert F. Kennedy

I would then ask my executives to provide a frank assessment of their individual leadership skills, style, and effectiveness, with particular emphasis on the following general areas:

(a) Working with people;

(b) Personality and character traits;

(c) Making decisions;

(d) Developing and selling ideas;

(e) Delegating responsibility.

The next step would be to compare their evaluations with the following criteria that I have personally established for these general areas.

Working with people

Working with your superior: Dependability and follow-through constitute two of the strongest measures of effectiveness in working with your superior. Initiative and doing more than expected make the best sales approach for a subordinate in building himself up in the eyes of his superior. It is always constructive to help the superior by supplementing his weaknesses, particularly when this can be handled with a reasonable degree of finesse and understanding.

Working with your associates: Make yourself easy to get acquainted with and to work with--loosen up--be adaptable. Be alert to your associates' attitudes--develop sensitivity. Learn how they react and what motivates them--develop objectivity. Show interest in your associates; seek advice from them, and go out of your way to help them.

Working with your subordinates: In working with subordinates, the necessary respect, prestige, and confidence to warrant acceptance as a leader must be earned. Such acceptance results from a consistent application of high personal standards and sound principles and from a good quality of decisions and ideas. A leader should seek the advice of his subordinates on problems and keep them posted on new policies and programs. He should help them to start new projects and carefully evaluate results of completed work. He should also outline their duties and responsibilities, preferably in writing, in terms which the subordinates can understand. Planning the work and having a program are great assets in effective leadership.

A leader should learn to inspire confidence and develop enthusiasm in subordinates. He should be a good listener, show a sympathetic understanding, and try to see the other fellow's viewpoint. He should keep the group "looking ahead" with a well worked out program. He should take an optimistic view whenever it is feasible and make subordinates comfortable when the "going is tough." He should show confidence by expecting much and letting subordinates know that he does expect much. He should compliment people when it can be done appropriately and sincerely, and he should, in fact, look for opportunities to do so.

Personality and Character Traits

I consider purposeful energy, progressiveness, intensity, and health as being particularly necessary to the successful leader.

Purposeful energy is commonly reflected in enthusiasm, initiative, and optimism.

Progressiveness is often reflected in the ease of generating and accepting new ideas.

Intensity and drive are characteristics of the outstanding executive which make him and his job almost one. A real leader reflects his job, and the job reflects his personality.

Health is a factor of growing importance. The requirements of leadership are becoming more exacting and complex, and the tempo continues to rise. The increasing frequency of hypertension, heart ailments, and stomach ulcers among executives, particularly those of middle age, should be viewed with alarm. More real relaxation, better planned vacations, and greater hobby interests are certainly desirable.

Making Decisions

Sound decisions are generally based on a combination of background knowledge, available facts, and exercise of judgment.

The knowledge element in decision-making is primarily derived from theories, principles, and practical experience. Good executives will coordinate, group, and use other people's knowledge for their mutual benefit.

The facts element is highly important in arriving at correct decisions. The ability to recognize facts, to know what facts are available in connection with each particular problem, to be able to assemble them, and then to analyze and interpret them, is fundamental to good leadership.

The judgment element includes drawing sound conclusions based on knowledge and facts. It involves thinking effectively--sifting the important elements of the problem from the superficial and exercising perspective.

Developing and Selling Ideas

A leader must get ideas easily. Hence he should try to develop his imagination. Ideas must first be obtained, then tested and timed for presentation, and finally sold to others for application.

Ideas usually originate from knowledge or research. I believe that every important office in my agency should continually apportion some of its time to research for new solutions and new ideas.

A leader must learn to sell ideas--to get his thinking across to others. One approach is to learn to write well organized, clear, convincing, and short memorandums. Another is to learn to conduct himself well in a conference, to go to a conference with a plan of attack, with suggestions and not just to sit in. And still another is to learn to speak to small and large groups; this not only builds personal prestige but is virtually a "must" for present and future leaders.

One should feel and express conviction in selling ideas. The old saying, "be sure you're right--then go ahead," certainly applies. At the same time, to avoid creating negative resistance, the degree of aggressiveness must be moderated by the proper amount of tact, finesse, and understanding.

Delegating Responsibility

A leader must be willing to delegate responsibility and to decentralize authority. You have to trust your people to do the job required. In working with subordinates, a leader should remember that one of the greatest human desires is to create or produce something, and to feel essential. Furthermore, as I previously stated, the higher your position is, the more dependent you become on others.

I truly believe that from the discussions generated in the "exercise" described above, leadership strengths and weaknesses can be identified and corrective actions can be taken to facilitate/promote effective leadership at my agency. If a leader develops his executives, he will in turn be even stronger. You can handle people more successfully "by enlisting their feelings than by convincing their reason."

WHAT'S THE GOOD (PASS)WORD?(U)

by [redacted] T4

DDT Senior Computer Security Coordinator

P.L. 86-36

A computer security compromise was recently discovered here at NSA, by an evaluation team from C1, the Computer Security Evaluation Center. The team was evaluating the computer at the request of DDT.

The compromise was the result of an administrative error. The system administrator had made a copy of the password file, which included the identifier and the encrypted password of all users of the system. However, the protection bits for the file were improperly set and the file could therefore be read by anyone on the system.

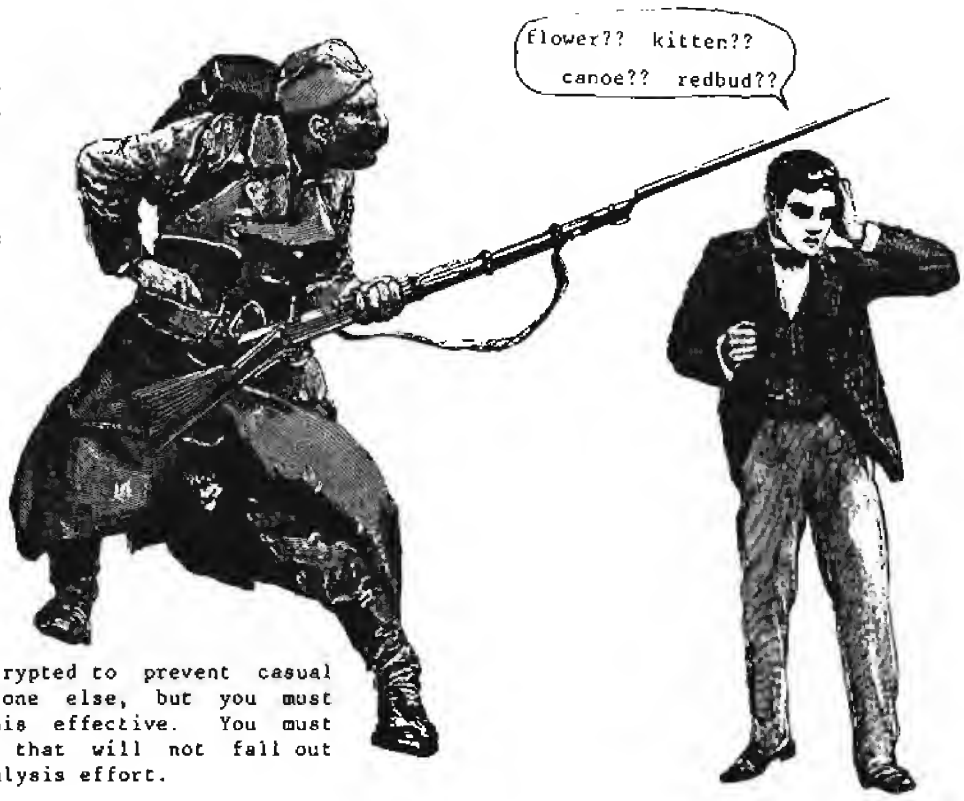
The evaluation team attempted to see how many passwords could be discovered from this file. They tried guessing passwords, sending them through the password encryption process to see if they matched: they recovered some passwords. The team then sent a dictionary of common words through the encryption process and compared the results: still more passwords recovered. Then the team tried all five letter values from aaaaa to zzzzz: in three days, they recovered a total of 107 of the 255 passwords in the file.

All users of the system have been directed to change their passwords, and the system administrator will be more careful about protecting the file in the future. In order to give the general user some idea of the kind of password that is easily guessed or discovered, the following is the list of passwords recovered by the team.

LIST OF RECOVERED PASSWORDS

abyss	escort
aesir	eyeball
again	fairway
apple	fishs
april	flower
backward	freedom
bandit	funny
barba	geisha
baseball	genie
beaver	golden
beetle	green
bible	happy
bingo	hawthorn
bluetop	holiday
brogue	horse
bushed	intel
candy	ironside
canoe	joewood
chance	kelly
check	kingfish
cjunk	kitten
confused	lambda
converse	landing
copper	lemon
crazy	locked
design	logic
digital	login
dogwood	lumpy
donna	major
drifter	michael
dumbo	mikey
eagle	mouth
elephant	muffin
empire	murphy

aroha	snowball
omega	softball
panel	saret
panelist	stage
perch	striper
permit	summer
pmrmd	sunshine
poets	susan
popcorn	tacos
puissant	testing
rabbit	tracing
radec	update
redbud	vision
romance	vkjrd
sailing	westward
scooter	wicks
scrabble	wildlife
security	window
shari	wizard
silver	



Passwords are encrypted to prevent casual recovery by someone else, but you must cooperate to make this effective. You must choose a password that will not fall out through a simple analysis effort.

The simplest factor you control is the length of the password. The longer the password, the better. If the password vkjrd in the list above had been one character longer, it would have taken about 26 x 2 1/2 days, or 65 days, to recover it.

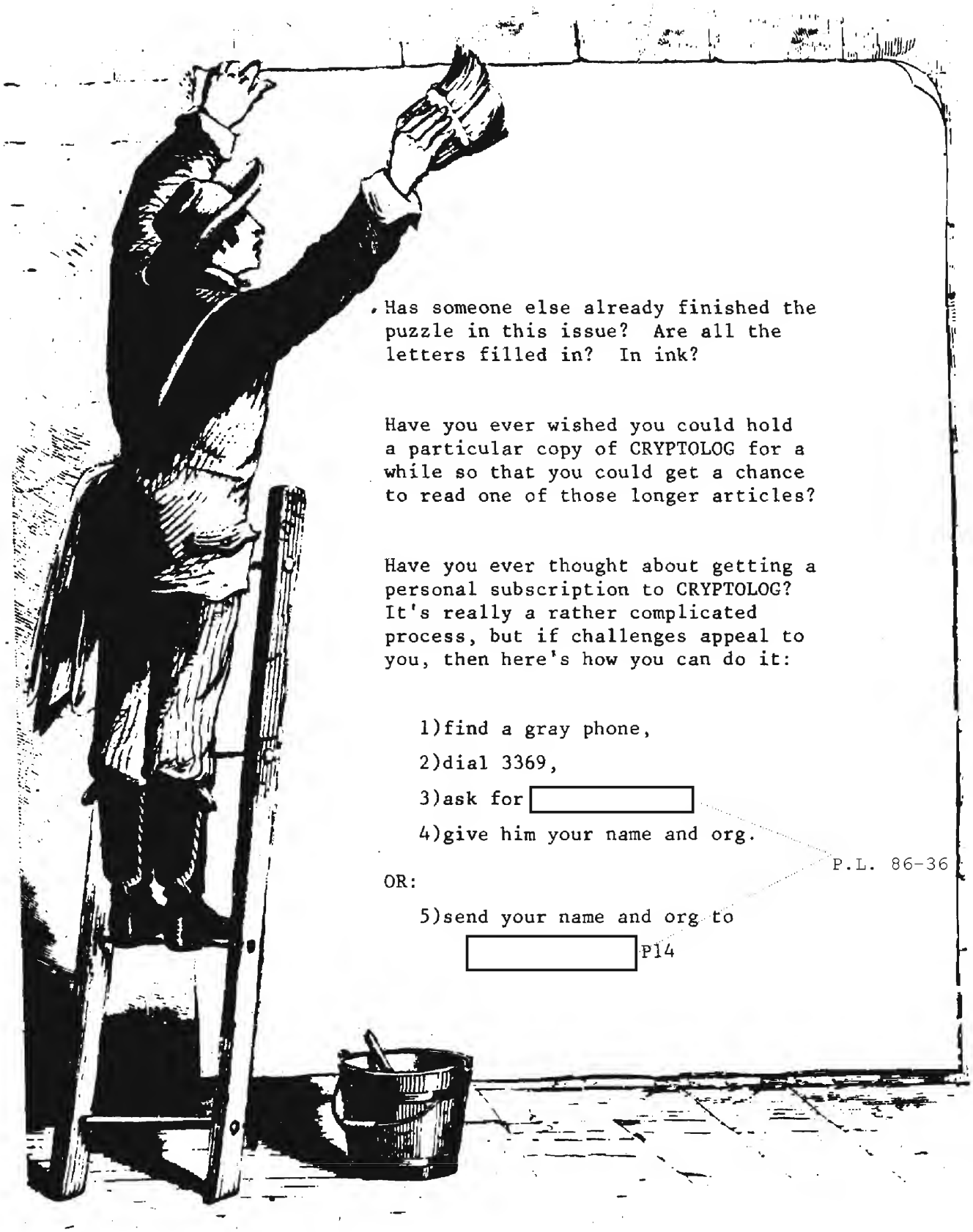
The table tells you that, if you use only a single lower case letter as a password, it can be recovered in, at most, 26 tries. If you use eight characters of lower case, upper case, numerics, and punctuation, then it could require 1,000,000,000,000,000 tries to recover your password.

A second factor that you control is the alphabet size. If you mix in both upper case letters and numbers, you increase the number of tries needed by the exhaustive method (i.e., trying every possibility). Note that there is not a single upper case character in the above list of recovered passwords.

A good password is eight or more characters in length. At least six different characters should be included. You should select uncommon words. Mixing in some upper case characters, along with numbers and punctuation characters, helps defeat discovery through exhaustive search.

EXHAUSTIVE TRIES NEEDED

	Alphabet Size	Password Length 1	2	4	6	8
Lower Case Letters	26	26	676	456,966	3.08×10^{8}	2.08×10^{11}.
Upper and Lower Case	52	52	2704	7.3×10^{6}	1.9×10^{10}	5.3×10^{13}.
UC, LC and Numbers	62	62	3844	1.4×10^{7}	5.6×10^{10}	2.1×10^{14}.
UC, LC, NR, Punctuation	75	75	5625	3.1×10^{7}	1.7×10^{11}	1.0×10^{15}.



Has someone else already finished the puzzle in this issue? Are all the letters filled in? In ink?

Have you ever wished you could hold a particular copy of CRYPTOLOG for a while so that you could get a chance to read one of those longer articles?

Have you ever thought about getting a personal subscription to CRYPTOLOG? It's really a rather complicated process, but if challenges appeal to you, then here's how you can do it:

1)find a gray phone,

2)dial 3369,

3)ask for [redacted]

4)give him your name and org.

P.L. 86-36

OR:

5)send your name and org to

[redacted] P14

HUMAN FACTORS: Text Editors (U)

by [redacted] P13

P.L. 86-36

REVIEW: HOW DO PEOPLE REALLY USE TEXT EDITORS?, J. Whiteside, et al, Proceedings of SIGOA Conference, Philadelphia, 21-23 June, 1982.

This study, carried out by five researchers at DEC (Digital Equipment Corp.), compared knowledge workers and secretaries performing their normal work with two different text editors. Keystroke statistics were gathered during normal usage of the editors. Both of the editors were screen editors. One, called EPT (Editor Prototyping Tool), was an experimental editor which contained a built-in keystroke logging facility. It permitted a simple set of editing functions, including cursor movement anywhere on the screen, search, text relocation, and text deletion. Text could be inserted or overprinted in modes activated by a function key. It did not offer the formatting functions included in most word processors, but it did provide automatic word wrapping. The other editor, WPS, was DEC's 200-Series commercial word processor. It was a character-oriented, screen editor in which editing was done on the bottom line of the screen. The cursor could be moved anywhere within the boundaries of existing text. It had logical equivalents for all EPT functions, but also offered many more functions, including sophisticated text-formatting.

Six knowledge workers were studied as they used EPT to create and revise their own reports and memos; they had at least three weeks experience with EPT before the test began. Eight secretaries provided the sample of WPS usage as they carried out their regular secretarial and administrative duties in a DEC R&D department. Their experience with WPS varied from one month self-taught to two years and three training courses. EPT keystrokes were logged by a built-in facility, while WPS keystrokes were captured by a PDP 11/34 computer. For both editors, the logging of keystrokes was accomplished in such a way that editor performance was not affected. Each keystroke was logged along with the time of occurrence.

The results of the study are highly interesting, and I believe they are directly relevant to our work situations. Neither EPT nor WPS is probably directly comparable to the text editors we use; EPT may be somewhat similar to the UNIX Rand Editor. Still, it seems probable that the essential editing functions (printing characters, cursor movement) are comparable across different editors. The methodology of the study has even more to offer than the results, in my opinion; I would very much like to see analyses of this kind carried out on many of our interactive systems, text editors and otherwise.

The data was first studied at the level of individual keys: What proportion of total keystrokes for all users was taken up by pressing each key? What proportion of the total time was used pressing each key? What was the average time per keystroke?

Transition probabilities were computed for pairs of keys: How likely is it that a user will press key B after pressing key A? The degree of randomness or organization in the pair transitions, and the degree of predictability in longer strings of keystrokes were studied in various ways. Finally, keystrokes were grouped into larger classes to provide a more global analysis in terms of "states," making it easier to compare results with different editors in terms of basic functionality for the user.

Here are some highlights of the results, adapted and simplified from the author's tables:

"Inactive" time was logged whenever no keystrokes occurred for a period of more than 150 seconds. The secretaries usually turned on their machines as soon as they came in in the morning and left them turned on all day, while the knowledge workers were using EPT on a time-sharing system and were less likely to leave the editor running when they weren't actually using it. The actual work hours and total keystrokes are quite comparable in the two samples; in fact, the six EPT users generated a few more keystrokes within slightly fewer work hours than the 8 secretaries. This seems highly interesting in itself. I would like to know more about this unexpected showing, in which six people who were not (presumably) trained typists but professionals doing their own documentation turned out more keystrokes in a shorter time than eight people whose primary task was skilled typing! Unfortunately, the paper does not address this point, so we are left in the dark about it. It may have been related to the text editors, in that WPS may have provided more power with special functions, so that the secretaries could accomplish more with fewer keystrokes. It raises a question about assessments of productivity based on keystrokes per person/hour, in any case.

CHARACTERISTICS OF USERS AND WORK SAMPLES

	EPT	WPS
Type of Editor	Simple Screen Editor	Sophisticated Commercial Word Processor
Users	6 Knowledge Workers	8 Secretaries
Total Person-Hours	212	482
Inactive Hours	127	390
Active Work Hours	86	92
Total Keystrokes	510,513	406,102

INDIVIDUAL KEYSTROKES IN EPT AND WPS

EPT		
KEY	% OF STROKES	% OF TIME
Print Char.	53.58	46.84
Left-Arrow	12.90	5.08
Right-Arrow	12.52	5.49
Delete	7.35	7.38
Down-Arrow	5.67	9.89
Up-Arrow	3.15	5.89
Return	1.38	4.38
Tab	1.01	1.66
Word	.34	.39
All Other	2.10	13.00

WPS		
KEY	% OF STROKES	% OF TIME
Print Char.	54.81	47.48
Advance	15.48	11.91
Line	10.30	6.27
Backup	6.59	7.41
Rub Char.	3.33	3.35
Return	2.83	8.08
Tab	1.52	1.79
Word	1.24	.65
Delete Char.	1.11	.90
All Other	2.79	12.16

Typing in characters accounted for a little more than half of all keystrokes, and nearly half of all time, in both editors. "Arrow" cursor movements in EPT accounted for about a third of keystrokes and a quarter of user time, while "Advance", "Line", and "Backup" (cursor-movement keys in WPS) accounted for very similar portions of keystrokes and time. Nine key types out of a total of 29 in EPT accounted for 98% of keystrokes and 87% of time, while nine key types out of a total of 64 in WPS accounted for 97% of keystrokes and 88% of time. Thus, even at the level of individual keystrokes, these two apparently quite different editors were used in a very similar way by two highly different sets of users. The authors of this paper summarize these results as follows: "A rough rule of thumb that emerges from our data is that free usage text editing consists of about 1/2 typing, about 1/4 cursor movement, about 1/8 deletion, and 1/8 all other functions put together. This rule has been shown to apply in two different situations: knowledge workers creating documents with an experimental text editor, and secretaries transcribing and updating documents on a commercial word processing system." (p. 37)

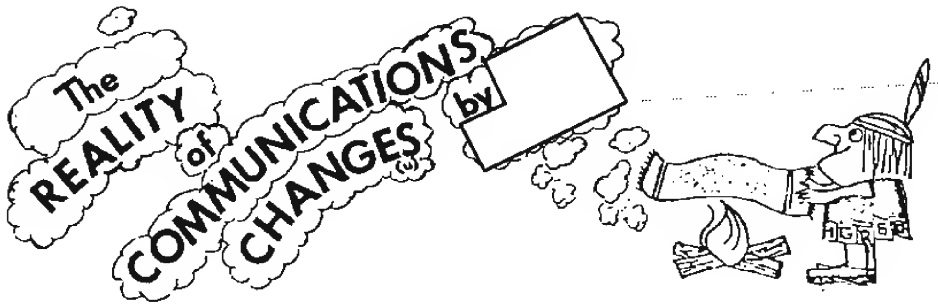
The grouping of keystrokes into states produces results that modify these proportions somewhat, as the table above shows. Typing uses up a bit more than half and cursor movement more than a third of the keystrokes. "Erasing" accounts four four times as many keystrokes as the "all other" category in both editors. It is interesting to note that the knowledge workers gave twice as much weight to "erasing" than the secretaries did. No explanation is offered for this difference in the paper. Perhaps the secretaries made fewer typing errors; on the other hand, the difference may be related to creation of documents by the knowledge workers. Composing an original document might be expected to call for more erasures than transcribing or updating a document originated by someone else.

I recommend this paper to all readers interested in human factors in our Agency. In my opinion, it represents the kind of well-designed, practical study we should be doing to obtain more hard data about user/system interactions in our offices.

STATES IN EPT AND WPS

	PERCENT OF KEYSTROKES	
STATE	EPT	WPS
Type	55.97	59.16
Cursor	34.39	34.45
Erase	8.27	4.44
All other	1.37	1.95

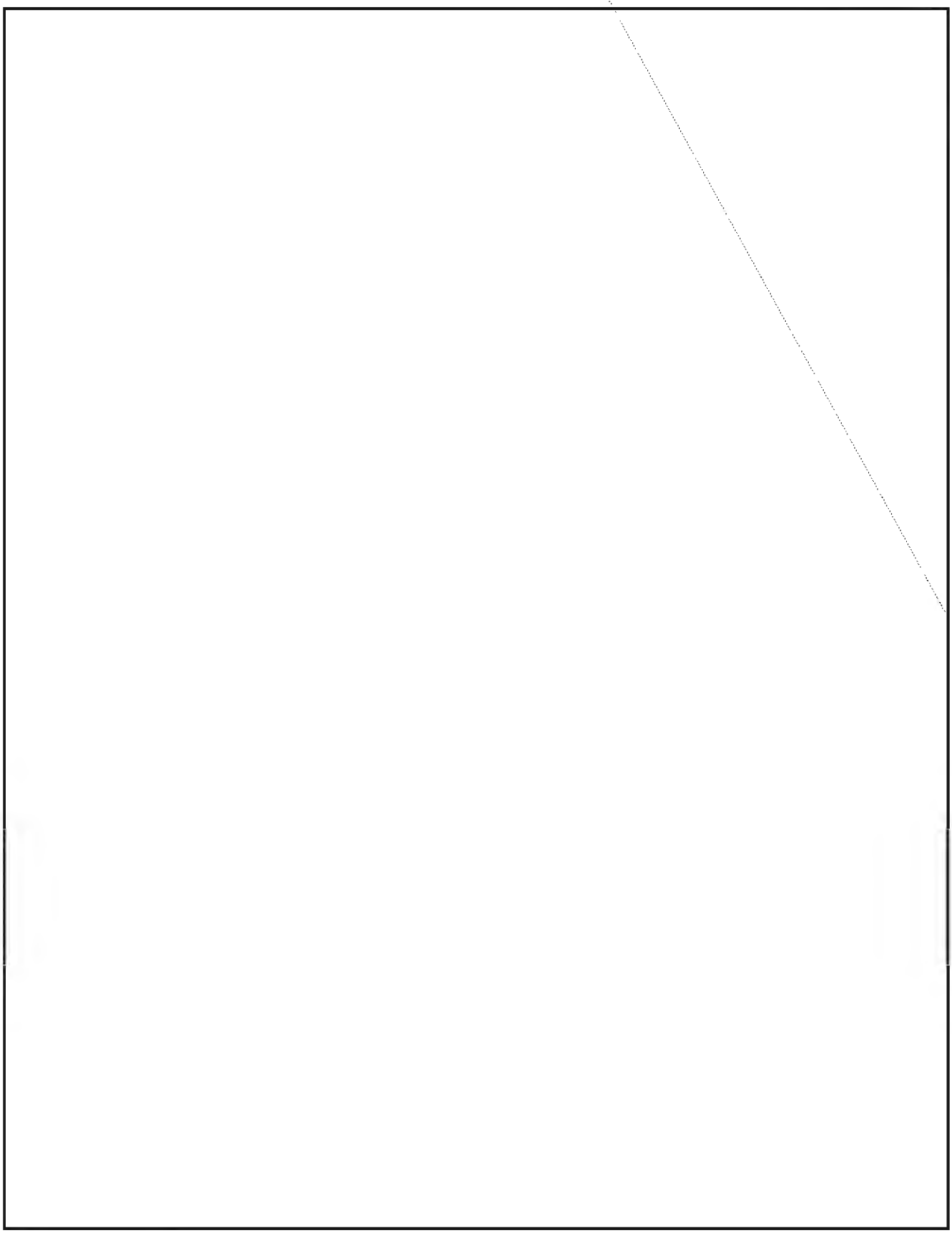
GOLDEN GLOW



P.L. 86-36

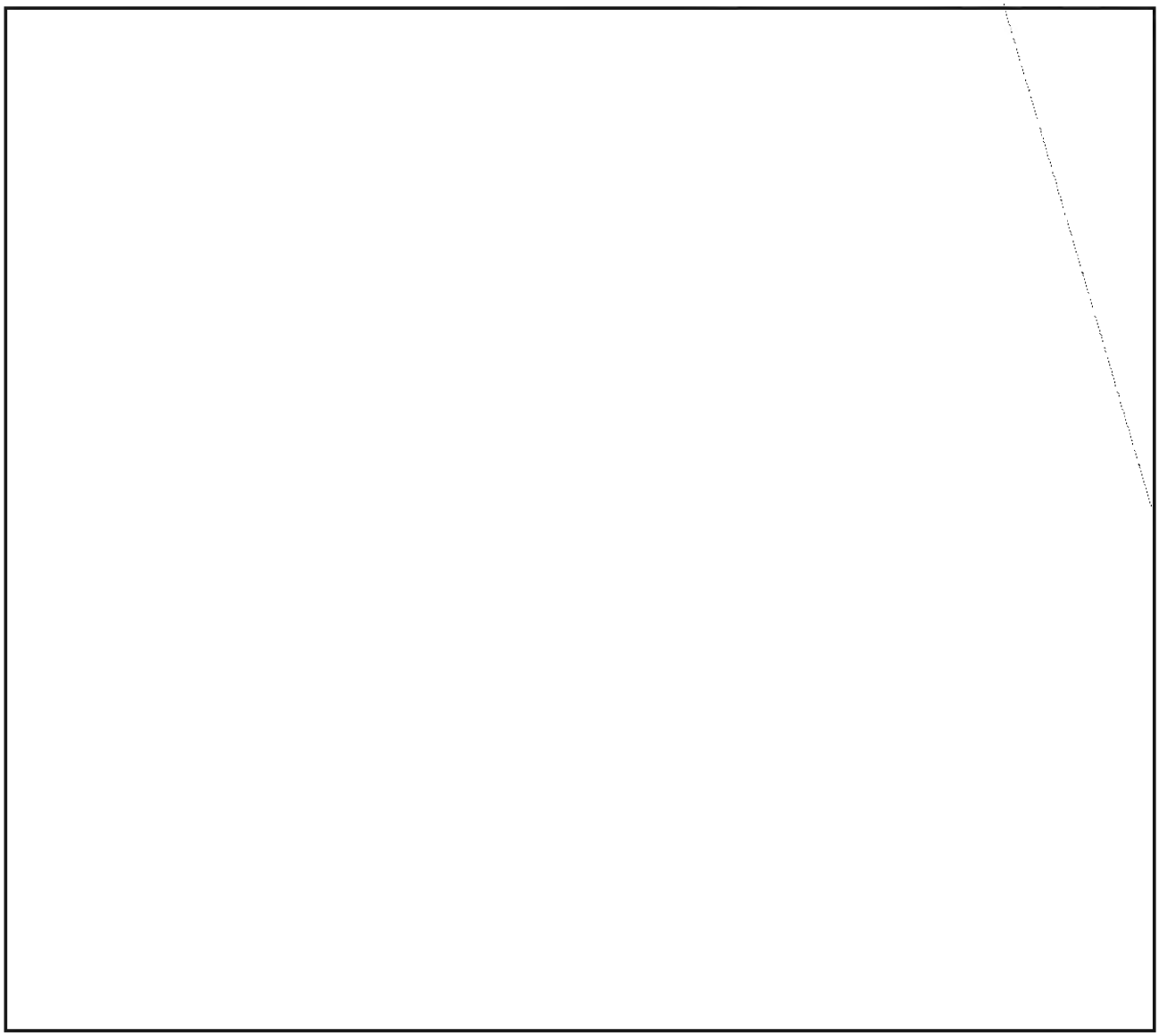
Reprint from DRAGON SEEDS, June 1972

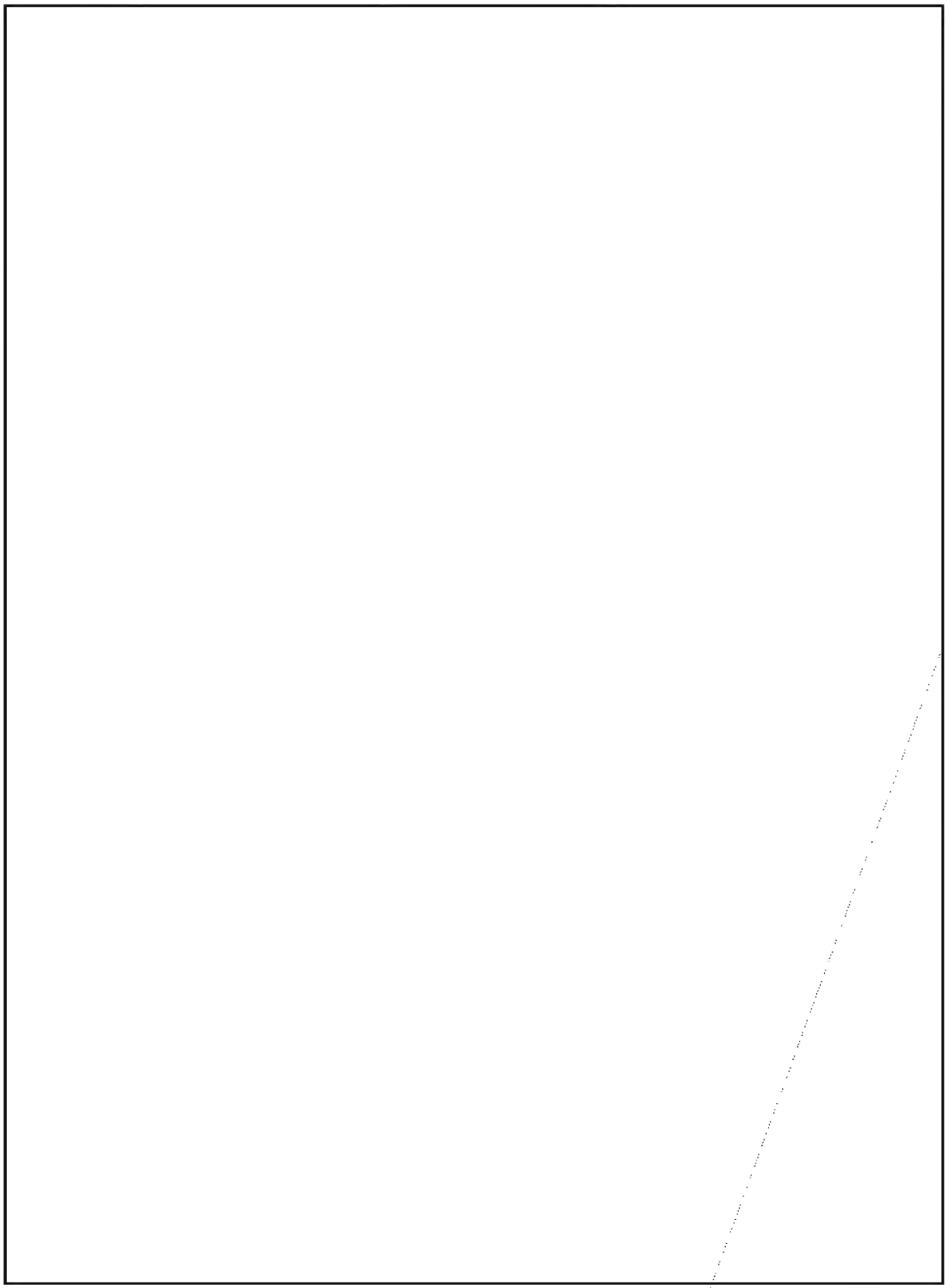
EO 1.4.(c)
P.L. 86-36



P.L. 86-36

NSA-Crostic No. 43





P.L. 86-36

SIGINT: 1990 (U)

Part 2

by [redacted] P13

OPTICAL FIBER

[redacted]

OPTICAL FIBER COMMUNICATIONS (NEC)

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in the second of several monthly installments, from his presentation at a January 1982 session of CA-305.

(U) Initial applications of optical fiber were for specialized applications, such as the communications circuits (see figure 21) that were installed with buried power cables. The fibers were unaffected by the powerful electrical fields, and gave reliable wideband circuits. Other specialized applications used the resistance to electrical noise and interference for shipboard and military applications, despite the fact that neither the glass nor the electro-optical components were very good.

(U) Rapid advances in glass technology and in laser and LED (light-emitting diode) and detector technology have occurred during the past ten years. These improvements have made short-distance circuits, e.g., within computer nets, economically feasible, and the telecommunication operators are beginning to install short-distance and medium-distance (up to a few kilometers). circuits in parts of the existing networks.

(U) By 1990 better glass and more reliable electro-optical components will make long distance trunks economical, and by the mid 1990's optical fiber loops will be introduced from the local switches to subscribers' premises. By 1982 the various Bell System companies had already installed over 25,000 miles of optical fiber trunk. A typical application will be the Northeast Corridor, a 400-mile trunk from Washington to Boston, using 3C digital transmission at 90 Mbps/fiber. Some fiber systems will use three separate light wavelengths at once, to give 270 Mbps/fiber. Typically an installed fiber system will have 12 fibers, with repeater spacing at 35 kilometers. Since coaxial cable repeater spacing is

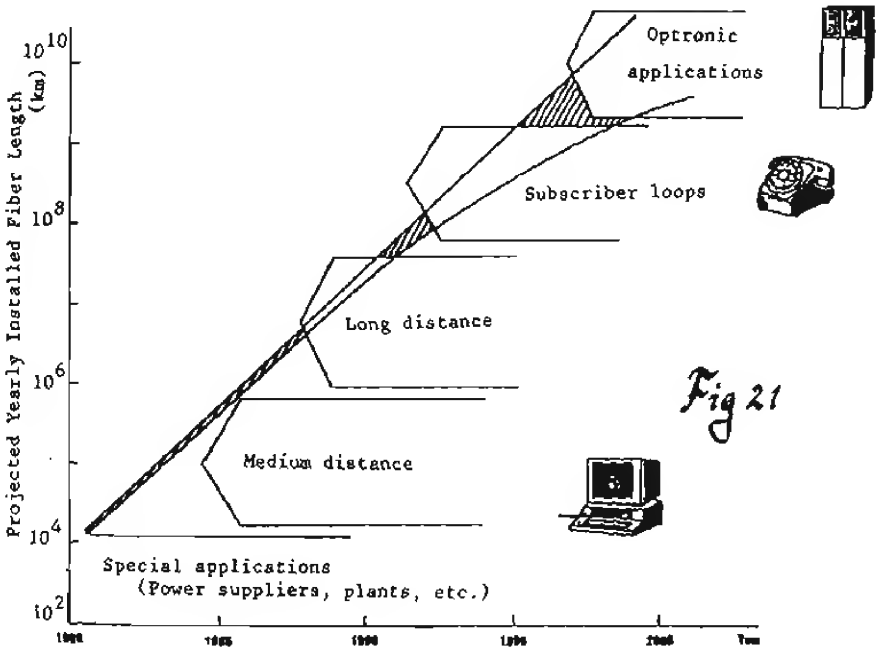


Fig 21

OPTICAL FIBER COMMUNICATIONS

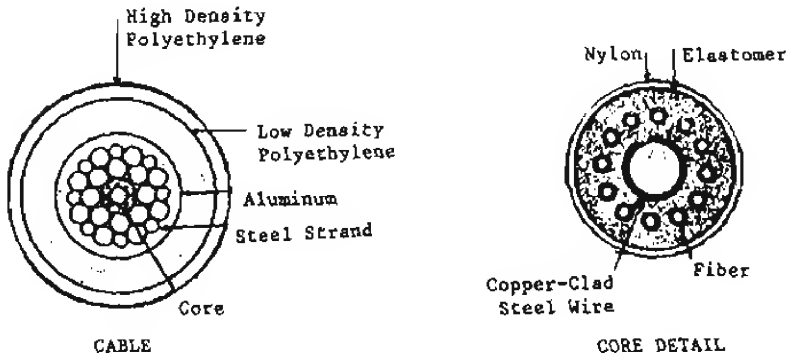


Fig 22 UNDERSEA FIBERGUIDE CABLE

about 4 km, the optical fiber offers big improvements in system design, maintenance, and cost.

(U) NEC predicts a million kilometers of installed fiber by 1985 and 100 million kilometers by 1990. Since the Japanese are among the world leaders in both the technology and the marketing, they are in a position to make this prophecy materialize.

UNDERSEA OPTICAL FIBER CABLE

(U) One of the most dramatic illustrations of the advances in optical fiber is the development of a transatlantic optical fiber cable (fig 22), to be operational by 1988, which will carry 72,000 two way voice channels between the U.S. and three foreign countries over a 6500-km undersea cable. Transmission bit rate will be 375 Mbps per fiber, and a TASI (Time-Available Speech Interpolation) will be used to triple the traffic capacity.

(U) Power will be supplied over a copper-clad central steel cable, and a dozen single-mode fibers will surround the core. SG cable repeaters will be used, with a regenerator for each fiber, spaced at 35 km. The system is expected to have a 25-year life. The first cable will probably be the start of a revolution in transoceanic communications, just as the first transoceanic coaxial cable began the explosion of transatlantic telephony.

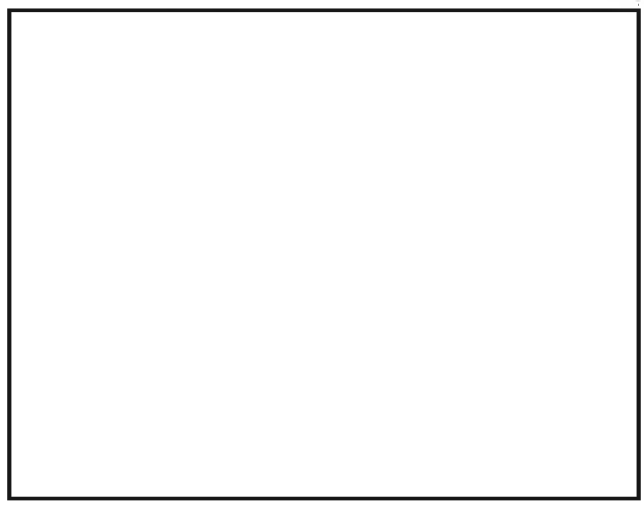
(U) While the AT&T undersea fiber trunk will use digital regenerators, the Japanese are now proposing a 5000-km undersea optical fiber cable with no regenerators, which will use linear optical amplifiers along the fiber. This will allow changes to the digital technology at the cable ends as technology improves. Experiments have already shown that power can be sent along light fibers to operate remote devices, so a completely optical system, with no electrical power or copper wire, should be feasible.

COST COMPARISON FOR UNDERSEA SYSTEMS

(U) Analysis by BTL has shown that, compared to the older 30MHz coaxial cable systems, the 274 Mbps optical fiber cable will give a 5-to-1 improvement in circuit costs. The very high bit rate will make special services such as video, video conferences, and data services feasible.

(U) While satellite technology will improve over the same time period, satellites are a stable technology, while optical fiber is still going through explosive growth in performance. The critical choke point in satellite communications is at the midocean points, where demand for spectrum and services is growing, while orbital and spectrum resources are fixed. The development of intersatellite links will relieve this problem to some extent, but in the long term the transoceanic capacity of optical fiber submarine cable--and its resistance to antisatellite weapons and electronic warfare--will make fiber the primary transoceanic medium. P.L. 86-36 EO 1.4.(c)

~~(S)~~ The impact on SIGINT of the development of transoceanic and overland optical fiber trunks is that traffic which now must go primarily by satellite will disappear onto fiber. The extreme publicity given to SIGINT over the past eight years by the revelations of World War II COMINT and by the excoriations of U.S. and British SIGINT agencies by governmental bodies, by journalists, by former employees, and by COMSEC and "communication protection" advocates, has made the telecommunication authorities highly conscious of satellite interception and microwave interception. Optical fiber will be a preferred transmission medium because it is so difficult to intercept.



BIGFON: OPTICAL FIBER LOCAL LOOP

(U) A number of European countries are now experimenting with applications of optical fiber to the local network. The BIGFON network (see figure 23) will be tested in several German towns over the next few years, to determine how various subscriber services are used. An optical fiber pair with a capacity of hundreds of millions of bits will run from the local switch to the subscriber premises, and will carry various two-way services, including telephony, television, facsimile, data communication, telex/teletex, and stereo reception. At the local switch, selected channels of video, stereo, etc., will be connected to the individual loop. Current estimates are that a fiber pair can carry three TV signals and a variety of other services.

(U) Glass quality and cost are important considerations, since the total amount of glass fiber will be large, replacing the copper wire loops of current local nets. Optical fiber glass is made primarily by two processes, viz: the crucible method which gives a cheap and stable method of producing low-quality glass (10 dB attenuation/km), and the MCVD (multiple chemical vapor deposit) method which gives a very flexible technique for producing high quality but expensive glass (0.2 dB/km loss). Expert opinion (Midwinter) expects industrial techniques to produce a stable low-cost glass at about 1 dB/km which will allow fairly long local loops. The better glass would also allow economical higher bit rates.

~~(C)~~ The effect of low-cost optical fiber local networks would be twofold, viz., a much wider range of services, including videophone and conference nets with high grade voice security at 64 Kbps, would be available in the local nets, and the plant would be cheaper and more reliable than the conventional copper wire networks, leading to expansion of local (urban) telecommunications services in less affluent countries.

(U) One of the main attractions of optical fiber local nets from the point of view of the PTT's is that over the air broadcasting could be almost eliminated, and this would put all information flow completely under the control of the PTT's.

GLASS PURITY

(U) The driving factor in the development of optical fiber communications has been the improvements in glass purity. In 1966 the first article proposing monomode waveguide operation of glass fiber was published, but the glasses available at that time made the proposal appear absurd because the attenuation was too high for any useful system. However blocks of pure silica were found commercially available with losses as low as 10 dB/km, and this spurred enormous progress in glass chemistry.

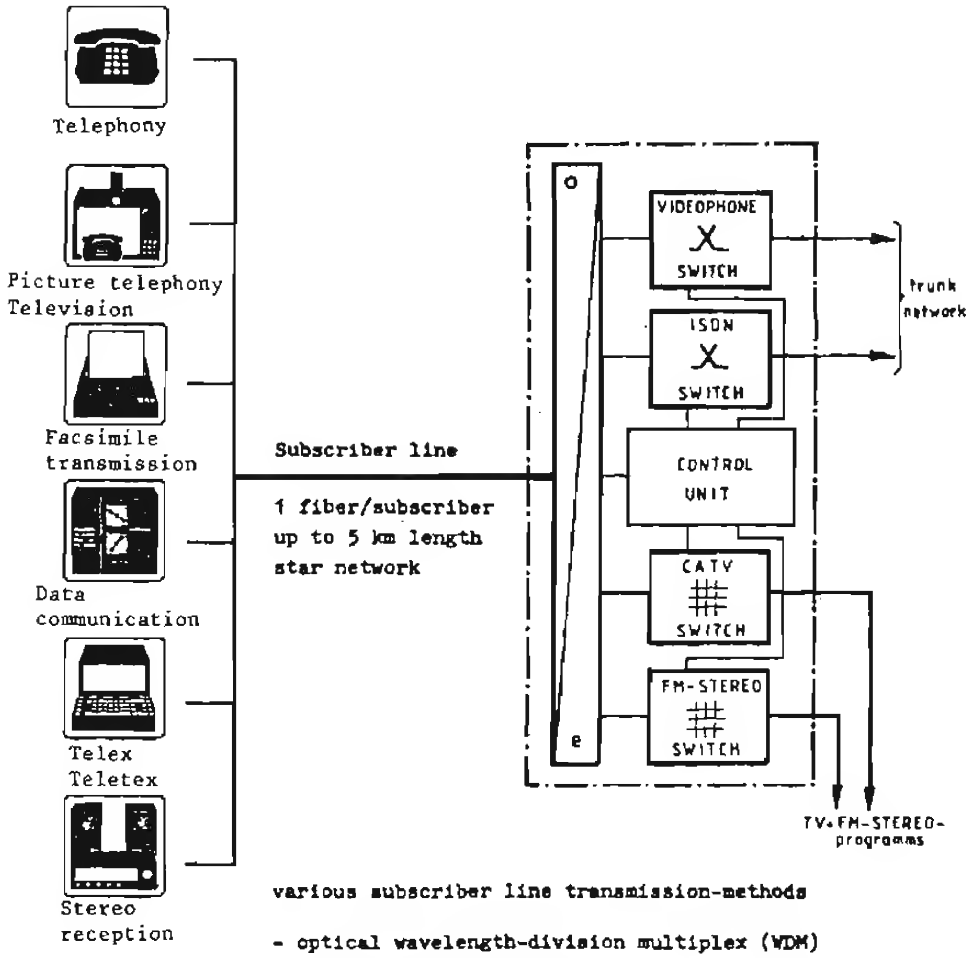
(U) The crude glasses of Egyptian times (3000 B.C.) had attenuation losses of 10 million dB/km, and over more than four millenia glass purity was gradually improved to the quality of Venetian glass of 1500 A.D. with losses of 10,000 dB. This represented a significant decline. Over the next 450 years, through the development of modern chemistry and industrial quality control, a further improvement was made to give the optical top quality glasses of 1970 with losses of 1000 dB per km. Then suddenly, in a decade of explosive development, completely new methods of purifying glass and drawing it into fibers were invented, with the result that a 10,000-dB improvement in glass attenuation was made in only ten years.

(U) The ratio of 10,000 dB corresponds to the number 10 raised to the power 1000, or a 1 followed by 1000 zeros, a truly phenomenal improvement.

(U) To visualize the effect of this improvement on optical communications, if all the power generating stations in the world converted all their power into light with perfect efficiency, and these many gigawatts of light were transmitted into a glass fiber with 1000 dB/km attenuation, then an observer one kilometer away would have to wait over a trillion years for the first photon to emerge. The glass fiber of course would be vaporized in an instant by the light absorption. By contrast, modern glass, at 0.2 dB/km loss, can transmit a few milliwatts of light 100 km without a repeater, at high bit rates over 100 Mbps.

BIGFON

broadband integrated optical fibre local telecommunications network



various subscriber line transmission-methods

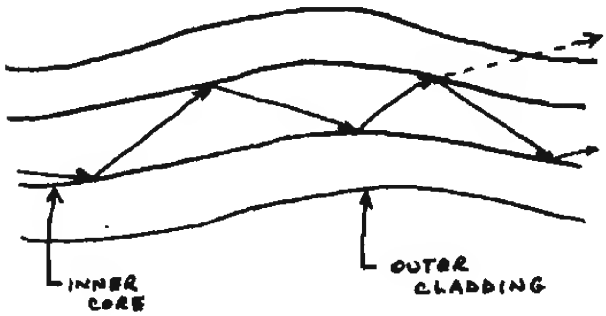
- optical wavelength-division multiplex (WDM)
- time-division multiplex (TDM)
- frequency-division multiplex (FDM)
- space-division multiplex (SDM)

Fig 23

ISS' 81 CIC Montréal 21-25 sept. 1981

(U) At the same time that the glass has been improved, the light transmitters and detectors have also been improved, especially in matters of lifetime and reliability. A few years ago the lasers and light emitting diodes had lifetimes measured in a few hours, but this has been improved to 100,000 hours, with further improvements to more than a million hours expected. Efficiency has also been improved so that very low power consumption will keep a long series of repeaters operating. This is important to submarine cables, where the repeaters are inaccessible.

(U) A comment about fiber manufacturing is in order because it implies certain limitations on SIGINT operations against different fibers. The manufacture of high-quality optical fiber is done primarily by two processes, viz., Modified Chemical Vapor Deposition (MCVD) and Vapor-phase Axial Deposition (VAD). Both MCVD and VAD produce a large glass rod that is subsequently drawn into very long fibers in a high-temperature furnace. A subtle chemical process known as thermopheresis is used to allow various chemical gases to penetrate into the hot glass while it is a tubular form turning on the lathe, and this process captures unwanted molecules and also deposits desired chemicals in a systematic way. The glass tube is then collapsed into a rod and drawn into a fiber. The lower-quality optical fiber is produced by a "double crucible" process in which a mixture of chemicals is put into two crucibles and melted, giving two kinds of glass of uniform composition but not as pure as MCVD yields. Glass from one crucible is allowed to gravity-feed into a thin fiber, and this is drawn through a gravity-formed tube of an outer glass, still in molten condition, to form coaxial fiber. The light travels in the inner fiber, and is reflected by the outer cladding.



24. MICROBENDING

(U) Because of the very high purity of the best glasses, the losses of light energy in propagation have been greatly reduced, but some losses still occur from a phenomenon known as "microbending," in which the light rays hit the interface between the inner and outer glass at a high enough angle so that some energy is transmitted into the outer cladding and escapes. The fibers are currently stored inside small-diameter plastic tubes so that they are not bent too sharply as the cables are laid around curves. The critical angle seems to be about six degrees. At higher angles of incidence microbending losses occur. In the design of the transmission systems, an allowance for such microbending losses is provided. The geometry of light propagation down a coaxial fiber is very complicated because of coupling between different propagation modes, so that the exact light path is unknown. In the graded-index fibers produced by the MCVD process, an axial focusing and defocusing of light takes place, but even that propagation is very difficult to describe. The result is that, in general, light energy is launched into one end of a lightguide and some of it emerges at the other, with random losses due to absorption, escape, etc.

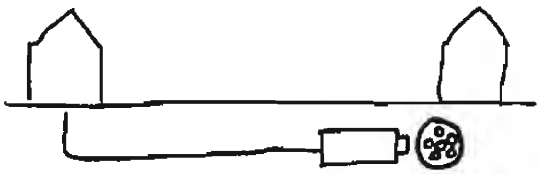
P.L. 86-36
EO 1.4.(c)

[redacted]

[redacted]

~~(S)~~ The central aim of optical-fiber SIGINT would be the concept of "proven reserves," derived from the petroleum and mining industries, rather than the current journalistic concept of hand to mouth immediate exploitation of whatever is easiest to get or fits current consumer requirements.

P.L. 86-36
EO 1.4.(c)



25. MOLE

[redacted]

[redacted]

[redacted]

systems, this after the fact access is not a workable scheme. If it took several years to get access to several fiber cables in an urban area, a crisis could come and go before any traffic could be collected.

~~(S)~~ The "proven reserve" concept does not only apply to interception, but to analytic and exploitation capabilities as well, so that the resources to attack and exploit systems should be developed and proved before there is a desperate need. Arguments that this is unaffordable should be evaluated by looking at the enormous success and wealth of the oil and mining companies, who do find this system affordable.

affects the entire SIGINT activity, rather than just hardening one problem at a time.

~~(S-CCO)~~ There is a historical precedent for this, in the World War II context, where the German traffic security, which at first thwarted Allied efforts at efficient collection, was solved for most of the war, and then at the end of 1944 became so secure that high-level cryptanalysis on the ENIGMA problem almost came to a halt because the traffic networks could no longer be identified or analyzed.

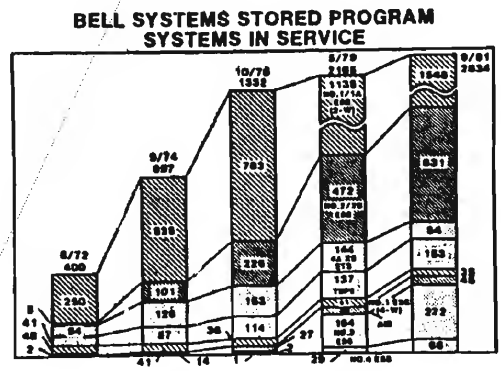
P.L. 86-36
EO 1.4.(c)

EVOLUTION OF EUROPEAN SWITCHING

(U) In the keynote papers at the International Switching Symposium in Montreal in 1981 (ISS 81), the rapid shift of the telecommunications plants of the Western nations from hard wired electromechanical switches to digital electronic switches was described. Although the old fashioned switches had been designed for a 30- to 50-year amortization, there is a growing trend to earlier replacement because the new switches are cheaper to operate and make more efficient use of the network. As a result, some 35 percent of subscriber loops will be connected to digital electronic switches by 1990, and 65 percent will be tied into the digital electronic switches by 2000.

~~(S)~~ As the new switches replace the old, the impact on SIGINT will be that the networks will become more flexible and efficient, and less rigid in the way traffic flows and in the services they provide. Some of the digital services, including those that use end-to-end encryption, will also have an impact on SIGINT.

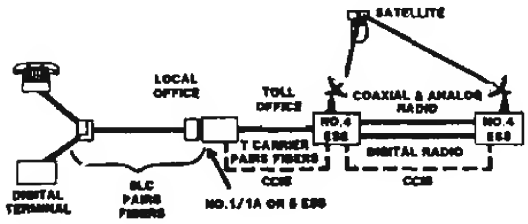
SWITCHING



26. BELL STORED PROGRAM CONTROL (SPC) SYSTEMS IN SERVICE

(U) In the U.S., the Bell System has also been very active in building and installing computer-controlled switches. Currently 47 percent of the local subscriber lines are covered by SPC switches, and the coverage in the Bell System by the early 1990's is expected to be 100 percent. There are now 2800 SPC systems in service.

(U) The SPC switches allow the network to provide new services, and also allow more efficient flow of traffic between switches.



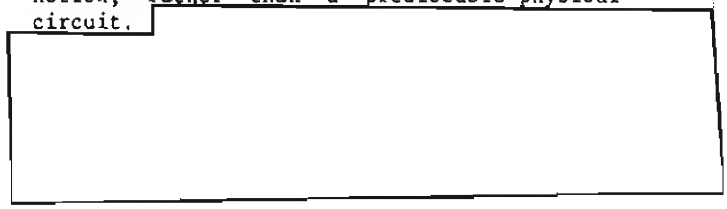
27. SWITCHED DIGITAL CAPABILITY

~~(S)~~ One of the significant changes in local services which the new switches will provide is high bit rate traffic over the subscriber loops. These high bit rates are made possible by the improvements in channel equalization and by sophisticated modems that can be implemented cheaply with the high density microelectronics. Some of the European nets are experimenting with 80 Kbps and 140 Kbps links, and the Bell System will offer 56,000 and 64,000 bps between the subscriber station and the local switch. Encrypted voice as well as facsimile and other data services will be available throughout the network where 1A ESS or No. 5 ESS switches are used. The Switched Digital Capability (SDC) will be introduced in 1984. For some subscribers, optical fiber will be used in the local loop. The 56,000 bps service will be end-to-end and will obviously provide high quality encrypted voice without the distortions that speech coders generate. This should lead to a rapid growth in encrypted voice for business traffic, with DES and Public Key interconnection between subscribers.

(U) Between the local switch and the toll switch, wireline or optical fibers will be used, under control of Common Channel Interoffice Signalling (CCIS). Coaxial cable, analog radio, digital radio, and satellite links will be used at the toll switches (No. 4 ESS), and CCIS signaling will be used where it is available. The CCIS information may flow over coaxial cable where the traffic itself flows over analog radio, digital radio, or satellite circuits.

~~(S)~~ The new Switched Digital Capability is an example of the new kinds of services which the digital electronic SPC switches will provide. In addition to the encrypted voice, encrypted high-speed (facsimile and electronic) mail and encrypted data services will flourish. Because the CCIS or other Common Channel Signalling will separate traffic addresses and routing from the traffic itself, the wideband transmission systems can be efficiently filled to capacity with a continuous stream of bits, or (in the case of analog radio links) successive talkspurts, without any indication of who the sender or recipient are. The toll switches are also capable of instantaneous automatic rerouting of traffic without any break in service, so that a given message or session may flow over various different channels. The effect is that the switches tend to act as transposition scramblers on relatively featureless and unidentifiable analog and digital traffic. The "dedicated" or leased channel will be a bookkeeping notion, rather than a predictable physical circuit.

P.L. 86-36
EO 1.4.(c)



Digital Switching
No.4 ESS

INTRODUCTION 1/16/76
• 67 offices now in service

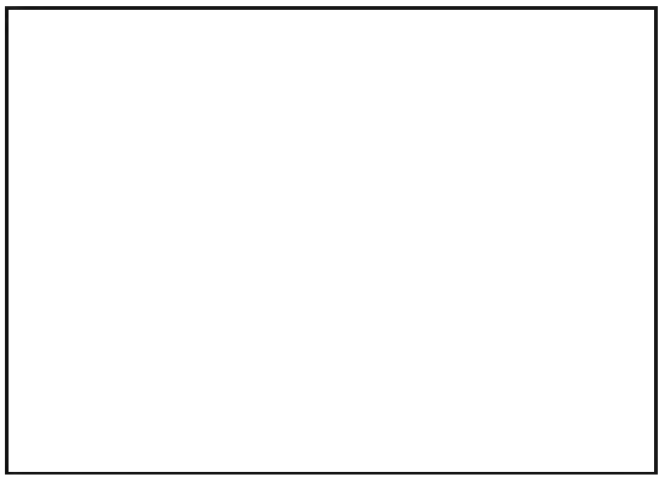
- **Characteristics**
  - **Time division switching network**
  - **Powerful central processor**
  - **New technology**
  - **Full duplication**
  - **Disciplined software methodology**
- **Features**
  - **Large capacity**
  - **Wide range of SPC network features**
  - **Extensive O.A. & M. features**

28. No. 4 ESS TECHNOLOGY

(U) At ISS 72, the No. 4 ESS created a sensation as a novel and ambitious functional and technological development. It was introduced into service in 1976 and 67 offices are now operating. However, the hardware technology of the switch has been completely replaced because of the technical superiority of newer microcircuits. No. 4 ESS uses time-division

switching in its internal logic, to give it very high resistance to "blocking" i.e., refusing a connection where a path actually exists in the switch.

(U) After the first shocking experience with switch software in the No. 1 ESS, the Bell System turned to disciplined software methodology, and now they can produce software which does not cause frequent switch outages. In spite of this, a new switch software product must "run in" for several hundred switch years before all the bugs are removed.



(U) The No. 5 ESS is a new local switch, designed to handle up to 100,000 lines, and designed to be used in rural areas. This switch applies time division switching to local nets. In contrast to the No. 4 ESS which is based on a powerful central processor, the No. 5 ESS architecture is based on distributed control. Powerful microprocessors are used in all of the peripheral modules, while the central processor performs more global control functions as well as overall administration and maintenance of the system.

(U) No. 5 uses modern software concepts, and all elements common to 512 lines are duplicated for reliability. An evolutionary plan has been set to provide a size range from very small to large offices of at least 100,000 lines with a large complement of customer, network, and administrative and maintenance features.

(U) The flexibility of the No. 5 ESS, and its production in various size ranges, is typical of the new developments in switching. The main producers of electronic switches are the French, Japanese, and L.M. Ericsson. The Swedish company produced a modularized AXE switch in the early 1970's, which in its original form routed signals in analog form, but was converted block by block to all digital operation. The first AXE switch was installed in Sweden in 1978, but has sold well abroad. Outside America there are only about 100 PTT customers for switches. The attraction of the AXE was that an analog network could be gradually converted to digital, and this technical lead enabled L.M. Ericsson to win the biggest telecom contract ever awarded, for a $5-billion Saudi telephone system. The conversion of existing analog networks over to digital operation, which involves the integrating of new switches into mixed analog and digital networks, is one of the most demanding problems in switch and network design.

P.L. 86-36
EO 1.4.(c)

ADVANCES IN TECHNOLOGY FOR ESS

- ■ VLSI
  - [] Microprocessors
  - [] Memory
  - [] Custom logic
- ■ Other Hardware
  - [] Optical fibers
  - [] High-voltage semiconductors
  - [] Display technology
- ■ Software
  - [] Architecture
  - [] Operating systems
  - [] High-level language
- ■ Development methodology
  - [] CAD
  - [] Program development support
  - [] Automated testing

(U) The switch designers have found it necessary to move into the forefront in development, manufacture, and application of the most modern hardware, design, and software technology. The network functions call for very complex logic, represented in VLSI hardware and software. Now the switch designers are converting software functions into "firmware" where the critical algorithms are designed in silicon from the start.

(U) Because of the high speed of modern

computers, various real-time telecommunications functions can be codified in higher level languages. Software has become a major part of switch and telecom plant production. At Bell Telephone Laboratories in 1950 no software was produced. Now half the staff works at software production. The advanced programming techniques enable software production at 100 times the rate of 15 years ago. The testing and debugging, and particularly the reliability of modern telecom software is a major technical factor. The other side of this coin is that once the software is designed and tested, it is very hard to change, because hundreds or even thousands of switches and transmission systems are made interdependent and interconnected by the software. Hence, even if the hardware is replaced, and parts of the software are codified into "firmware," the basic software system will probably have a long operational life. The software programs are often very large, running into hundreds of thousands of lines of code, and the developers are frequently protective of their "source level" program scripts.

[redacted]

[redacted]

[redacted]

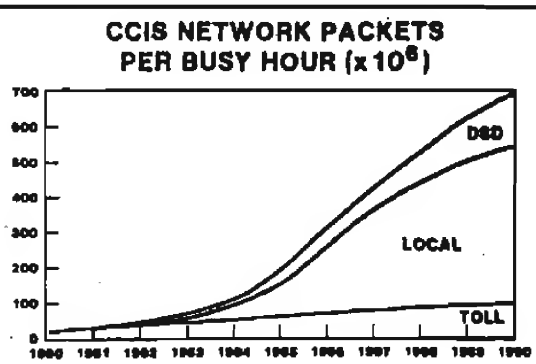
COMMON CHANNEL SIGNALLING

(U) In Common Channel Signalling the addressing information used to specify the call and the routing is not sent as a prefix on an idle channel. Instead, a separate dedicated channel is used to carry all the addressing and routing and signaling data. The result is that the transmission facilities are used more efficiently because idle channels do not have to be held open for some minutes while successive channels are found, and then until a called party finally picks up the telephone. On long distance calls, signaling and call setup used to take about half the channel time. The application of common channel signaling allows network efficiency to be practically doubled without building new plant.

P.L. 86-36
EO 1.4.(c)

(U) Three major systems are No. 6 CCITT, No. 7 CCITT and the Bell System CCIS Common Channel Interoffice Signalling.

[redacted]

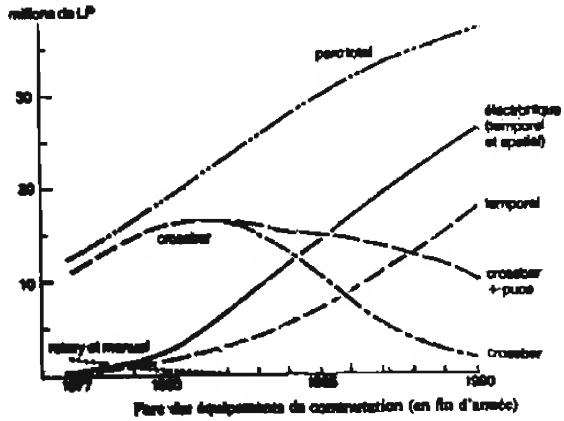


30. CCIS NETWORK PACKET TRAFFIC FORECAST

(U) In the Bell System, Common Channel Signalling is already in use between some switches and a packet network is employed to transmit the switching data. Currently some 20 million packets are sent during a peak hour. By 1990 the packet traffic rate for CCIS will rise to 700 million packets per hour. The dedicated CCIS packet network operates to set up the circuits switched network that will actually carry the traffic.

(U) While the new digital switches can be designed to implement common channel signaling, the older electromechanical switches, e.g., crossbar, are designed around a control system that uses in-channel prefix signaling. The French have developed an innovation for this problem called PUCE, which will retrofit an SPC computer into existing crossbar switches so that the crossbars can be controlled by common channel signaling. This will enable the entire French switched network to be operated by common channel signaling. The PUCE retrofit will allow the existing switches and transmission facilities to be operated more efficiently, without the expense of replacing the existing large investment in electromechanical equipment. This will also prolong the life of the crossbar plant. A plan published by CNET shows the effect of PUCE in extending the life of crossbar switches.

P.L. 86-36
EO 1.4.(c)



31. FRENCH SWITCHING EQUIPMENT ASSETS

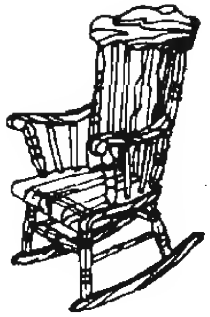
(U) The major growth will be in time-division electronic switches (temporel), with rotary and manual phaseout by 1983, and ordinary crossbar dwindling after 1984. The crossbar with the PUCE retrofit will remain at a fairly steady level up to 1990, presumably as a result of converting the ordinary crossbars.

(U) Summing up the switching trends, time-division has the greatest growth potential, and the wide use of time-division digital switches will reduce switching from 50 percent to 20 percent of total plant value, but many

years will pass before most countries can afford this. On the other hand, the low cost and high reliability of microprocessors and computers will make it increasingly attractive for PTT's to seek cheap retrofits and hybrid systems which will give more efficient operation and more or newer services, without the expense of replacing still serviceable equipment.

(U) In most poor countries, the problems of maintaining outside plant will be as significant a factor as shortage of money in retarding the successful introduction of digital electronic switches; defects and noise in the outside plant (subscriber loops and trunk transmission) cause errors that can disable the more critical digital technology. Another key factor in the introduction of digital switches in any country is the distribution of timing standards, because close synchronization through the networks is needed. This is already a problem in the U.S. where different suppliers provide equipment to hundreds of "independent" operating companies. Once a small country starts to introduce digital switches, the difficulties of time distribution and digital interface will cause special problems for any rival manufacturer who wants to sell in that market.

P.L. 86-36
EO 1.4.(c)



ANSWER: An Old Problem (U)
(CRYPTOLOG, August 1982)

When you finish, send up a flare!

EO 1.4.(c)
P.L. 86-36

Not
Secret
Anymore

P.L. 86-36

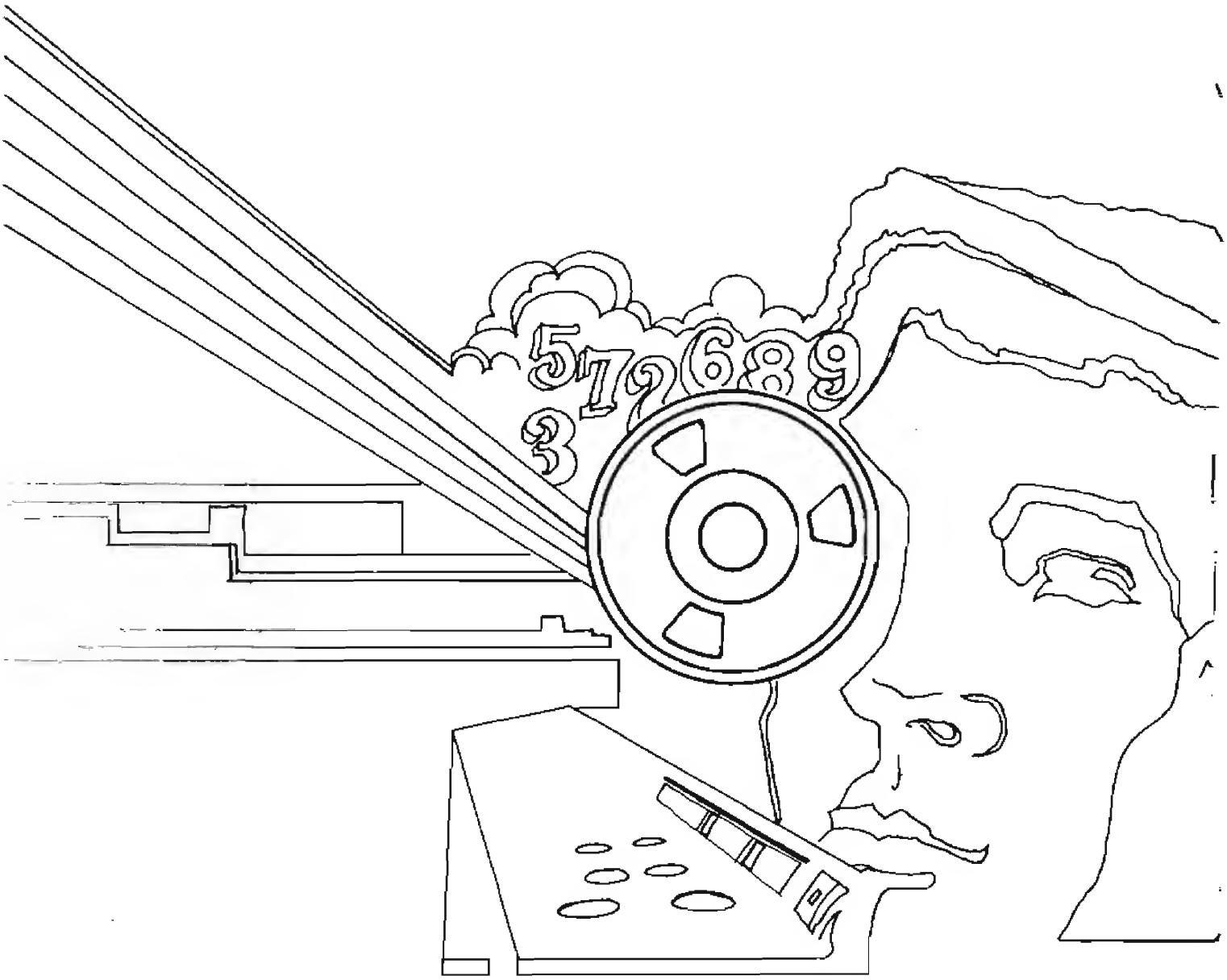
(U) May I add a few words to [redacted] reminiscences in the August 1982 Cryptolog, especially to his comments about the initials NSA standing for "Not Secret Anymore"? Like Brother [redacted] I recall those days of "M&M" (as we lovingly called Martin & Mitchell) and I also remember figuring out that expansion for myself, but I doubt if I was the only employee to come up with the clever meaning for "NSA."

(U) I remember including a cartoon in my book NonseNSA, showing President Eisenhower denying everything that M&M had said, ending up with, "and there is no such agency as NSA at Fort Meade, Maryland. In fact, there is no such place as Fort Meade, Maryland!" and scribbling on the bottom of the page "NSA now stands for 'Not Secret Anymore!'" Unfortunately, I loaned NonseNSA to [redacted] who used 2 or 3 cartoons from it in early issues of Cryptologic Spectrum and then retired without returning it to me, so I don't know if the book is still in existence.

(U) But at least I'm glad to see that somebody else used "Not Secret Anymore" since my other great discovery about what an agency's initials meant seems to have been restricted to me alone. When President Reagan appointed William J. Casey to be the head of CIA and then got our Admiral Inman to be his deputy, I remarked on several occasions that the CIA was "the Casey-Inman Agency" (which I thought was pretty clever--in fact, I was tempted to send it in to "The Ear" at The Washington Star--but to date I've never heard or seen it used by anyone but little ol' me...and now that Admiral Inman has left, I doubt if I ever will).

[redacted] P16

P.L. 86-36


5726893